PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :
E05B 49/00, G08B 29/00
G06K 19/00

A1

(11) International Publication Number: WO 90/15211

(43) International Publication Date: 13 December 1990 (13.12.90)

(21) International Application Number: PCT/AU90/00235

(22) International Filing Date: 4 June 1990 (04.06.90)

(30) Priority data:
PJ 4535 2 June 1989 (02.06.89) AU

(71) Applicant *(for all designated States except US)*: TLS TECHNOLOGIES PTY. LTD. [AU/AU]; Unit 7, 170 Forster road, Mount Waverley, VIC 3140 (AU).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)* : HARRIS, Robert, Jackson [AU/AU]; Unit 7, 170 Forster road, Mount Waverley, VIC 3140 (AU). SHAW, Harold, Malcolm [AU/AU]; Unit 7, 170 Forster Road, Mount Waverley, VIC 3140 (AU).

(74) Agents: BRETT, Noel, T. et al.; Griffith Hack & Co., G.P.O. Box 1285K, Melbourne, VIC 3001 (AU).

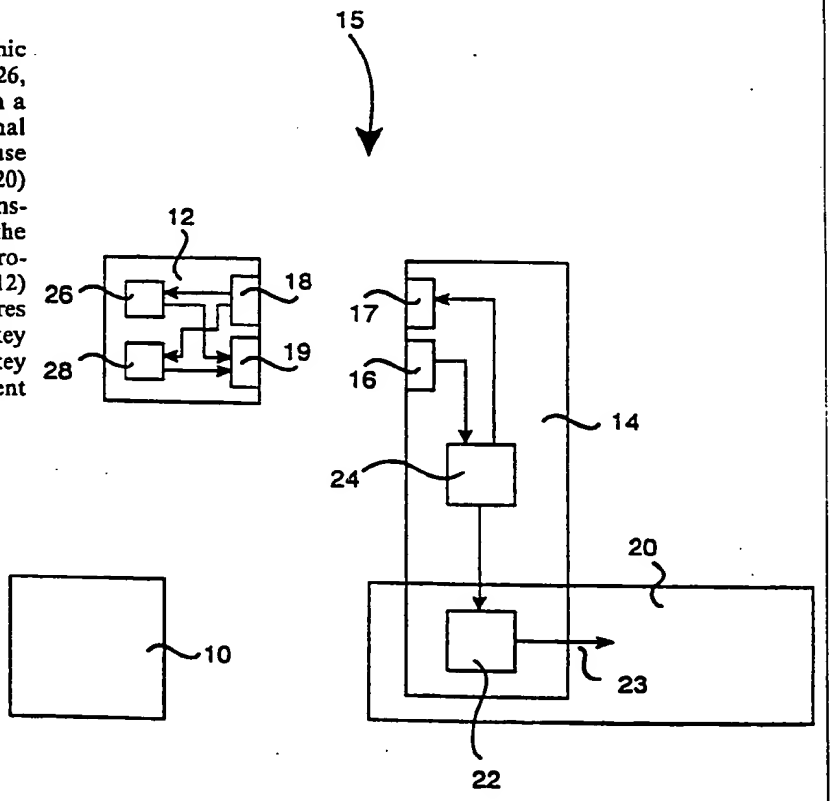
(81) Designated States: AT, AT (European patent), AU, BB, BE (European patent), BF (OAPI patent), BG, BJ (OAPI patent), BR, CA, CF (OAPI patent), CG (OAPI patent), CH, CH (European patent), CM (OAPI patent), DE*, DE (European patent)*, DK, DK (European patent), ES, ES (European patent), FI, FR (European patent), GA (OAPI patent), GB, GB (European patent), HU, IT (European patent), JP, KP, KR, LK, LU, LU (European patent), MC, MG, ML (OAPI patent), MR (OAPI patent), MW, NL, NL (European patent), NO, RO, SD, SE, SE (European patent), SN (OAPI patent), SU, TD (OAPI patent), TG (OAPI patent), US.

Published
With international search report.

(54) Title: SECURITY SYSTEM

(57) Abstract

A security system (15) is described. An electronic key (12) contains user codes in user code registers (26, 28) which, if determined to match a code installed in a code register (24) of a key reader (14) during a normal operation of the key (12) with the key reader (14), cause issuance of a control signal (23) to a secured means (20) to enable a change of secured state thereat. Data transfer of the codes between the electronic key (12) and the key reader (14) is contactless. A key coder (10) can provide for recording the code of the electronic key (12) with a new code by a user of the system, which requires subsequent steps to provide the new code to the key reader (14) such that the electronic key (12) and the key reader (14) will then be code matched for subsequent operation of the system.



* See back of page

DESIGNATIONS OF "DE"

Until further notice, any designation of "DE" in any international application whose international filing date is prior to October 3, 1990, shall have effect in the territory of the Federal Republic of Germany with the exception of the territory of the former German Democratic Republic.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MC	Monaco
AU	Australia	FI	Finland	MG	Madagascar
BB	Barbados	FR	France	ML	Mali
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Fasso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GR	Greece	NL	Netherlands
BJ	Benin	HU	Hungary	NO	Norway
BR	Brazil	IT	Italy	RO	Romania
CA	Canada	JP	Japan	SD	Sudan
CF	Central African Republic	KP	Democratic People's Republic of Korea	SE	Sweden
CG	Congo			SN	Senegal
CH	Switzerland	KR	Republic of Korea	SU	Soviet Union
CM	Cameroon	LI	Liechtenstein	TD	Chad
DE	Germany, Federal Republic of	LK	Sri Lanka	TG	Togo
DK	Denmark	LU	Luxembourg	US	United States of America

SECURITY SYSTEM

Field of the Invention

This invention relates to a security system and relates particularly, but not exclusively, to a coded proximity key and reader system and parts thereof.

Background of the Invention

As an improvement over conventional lock and key systems, it is known to provide electronic security systems which operate by a user inputting a secret code on a keypad or the like. Examples of such systems

include the familiar Personal Identification Number (PIN) authorisation common in banking transactions and in certain domestic appliances such as video recorders or car radios. The PIN system is open to abuse if the PIN is divulged or discovered by another party.

Other more recent security systems have included the card-type of actuating key, where a plastic card is encoded with a code on a magnetic swipe or strip. This code is read by passing the swipe past a magnetic sensor. Such codes can be easily read in an unauthorised manner, and lead to fraudulent use.

Some card-keys also contain microprocessors, which allows certain functions to be communicated between the key and the reader, for example, allowing recoding by substitution of another code. The disadvantage of these card-keys is that the particular contact required to be made between the key and the reader is open to contamination or vandalism.

A most recent development has been proximity card-keys, which are operated by bringing the key within a defined distance of a reader but not requiring contact therebetween, such that a code contained within the key can be transmitted to the reader. These systems can be of a number of types including some which require a power supply integral with the key, and others which receive power from the reader in order to permit the code contained in the key to be transmitted.

Security systems have as a fundamental consideration the need to maintain integrity and to minimise the opportunities for abuse of the system. It is desirable to design a security system which minimises the potential for any of these such weakness to be exploited.

Conservative security strategies are based on the assumption that at some time all invariant parts of a system will become known to potential attackers, so it is

necessary and desirable to design the variable parts of a system with a high degree of security. Particularly, codes for individual users of a security system are vulnerable, and there is a need for the facility to change such personal codes if it is thought that a code has become known to some other party.

Summary of the Invention

It is an object of the invention to attempt to overcome one or more of the disadvantages in the prior art.

Therefore, according to one aspect of the invention there is provided a security system comprising:

a key reader including a signal output means, a signal transmitter, a signal receiver, and a code register for storing an installed code, at least a part of the key reader being integral with a secured means and for providing a control signal thereto from the signal output means to change the secured state of said secured means;

(b) an electronic key including a signal transmitter, a signal receiver and two user code registers, a first of the registers being for storing an initial code and the second of the registers being for storing a new code;

the system being operable such that when said key transmits data representative of said initial code to said reader and there is then provided a match between said initial code and said installed code, there will be generation of said control signal from the signal output means to change the secured state of the secured means,

and further being operable such that if said key transmits data representative of said new code to said reader and there is no match between said new code and said installed code, said key can then receive a request from said reader via said signal receiver to

tansmit data representative of said initial code to be received by said reader, and if a match is then provided between said initial code and said installed code, said reader will be placed in a mode to substitute said new code for said installed code to form a next installed code, so that following substitution, the system will be code matched.

According to a further aspect of the present invention there is provided a method of operating a security system having an electronic key and a key reader, to cause a change of a secured state of a secured means, the method comprising the steps of:

(a) encrypting data representative of an installed code present in said reader,

(b) transmitting said encrypted data representative of said installed code from said reader,

(c) receiving said encrypted data representative of said installed code at said key,

(d) decrypting said received data,

(e) encrypting said decrypted data to form encrypted data representative of an initial code present in said key,

(f) transmitting said encrypted data representative of said initial code from said key,

(g) receiving said encrypted transmitted data at said reader,

(h) decrypting said received data,

(i) comparing said decrypted data representative of said initial code with said data representative of said installed code, and

(j) if there is a match, causing generation of an output signal to the secured means to cause the change of its secured state.

Preferably, the method comprises the further steps of manipulating the received decrypted data in the key following step (d), and manipulating the received decrypted data inthe reader following step (h).

According to yet a further aspect of the present there is provided a method of operating a security system having:

an electronic key and

a key reader which in a normal operation can provide an output signal to a secured means in response to there being code matching between an initial code stored in the key and an installed code stored in the reader whereby the secured means can change its secured state,

the method comprising the steps of:-

(a) providing a new code to said key so said key has both said initial code and said new code,

(b) transmitting data representative of said new code from said key,

(c) receiving the data representative of said new code at said reader,

(d) determining if there is a match of said new code with said installed code,

(e) on a mismatch, causing transmission of data representative of said initial code to said reader from said key,

(f) receiving the signal of said initial code at said reader,

(g) determining if there is a match of said initial code with said installed code,

(h) on a match, placing said reader in a mode to substitute said installed code with said new code to form a next installed code,

(i) and thereafter upon operation of the system with the new code, causing said output signal to be provided upon a match with said next installed code.

According to a further aspect of the present invention, there is provided a key for a security system, said key comprising a signal transmitter, a signal receiver and two user code registers, the first of the registers being for storing an initial code and the second of the registers being for storing a new code, and circuit means for permitting said initial code to be replaced by said new code, said circuit means including a comparator and gate means connected therewith, said comparator being for comparing the initial code with a code received by said receiver and upon a match being determined, enabling said gate means so said initial code in said first register will be passed to said second register, said transmitter being operable to transmit data representative of the initial code in said first register for normal operation of said key.

Brief Description of the Drawings

Examples of preferred embodiments will now be described with reference to the accompanying drawings, wherein:

Figure 1 shows a simplified example of an embodiment;

Figure 2 shows detail of the key recoding proceudre;

Figure 3 shows further detail of the data transmission process in the example of Figure 1;

Figure 4 shows an example of the bit composition of a data word contained in a key;

Figure 5 shows a flow diagram of the key recoding operation; and

Figure 6 shows a flow diagram illustrating steps in the normal operation of the system of Figure 3 including the code changing operation.

Description of Preferred Embodiments

Embodiments of the present invention have application to security access systems, mechanical and electrical services in buildings and industrial complexes, anti-theft systems, and for the prevention of illegal use of appliances or other electrical goods of value so as to decrease their value if stolen. Other applications, not specifically mentioned, are equally applicable.

Figure 1 shows a simplified general configuration of an example of the invention which relates to a security system suitable for an automobile, and particularly operating as an anti-theft device.

In this example, the system 5 comprises three main components, being an electronic key 12, a key reader 14 and a secured means 20. The key reader 14 is, in part, integral with the secured means 20, having a signal output means 22 providing a control signal 23. The secured means 20 in the example described is the electronic ignition for a motor vehicle. The control signal 23 is such as to enable the electronic ignition hence to allow the vehicle to be started.

The key reader 14 is also provided with a code register 24 having an installed code therein. The code register 24 is in communication with the signal output means 22, and with a signal receiver 16 and a signal transmitter 17.

The secured means 20, as the electronic ignition, may be manufactured with the signal output means 22 as an integral component, else the signal output means 22 may be retrofitted in such a way that it can not be bypassed easily. It is necessary for security that a part of the key reader 14 be integral with the secured means 20, and it is equally applicable to provide only the signal receiver 16 and the signal transmitter 18 separate from the electronic ignition.

The electronic key 12 comprises a signal receiver 18 and a signal transmitter 19 which can pass signals respectively to or from either one of user code registers 26,28.

If it is assumed the key 12 has an initial code stored in one of the user code registers 26,28 which, as the current code, matches the installed code stored in the code register 24, then it is convenient to describe in detail how normal operation is performed so as to provide the control signal to change a security state of the secured means 20. That is, in this embodiment, on a match between the initial code and the installed code, the electronic ignition of the motor vehicle will be enabled.

The owner firstly enters the vehicle and holds the key 12 near the location of the signal transmitter 17 of the reader 14 which would conveniently be located near the ignition switch. The transmission is therefore contactless, requiring only that the key 12 and the reader 14 be proximate to each other.

When the key 12 comes into proximity with the transmitter 17, a signal representative of the initial code (as the current code) is transmitted by the signal transmitter 19 and is received by the signal receiver 16. If there is a match between the initial code and the installed code, the signal output means 22 causes the control signal 23 to be generated to enable a change of security state enabling the electronic ignition, such that the vehicle can then be started.

This is a simplified discussion of the normal operation of the system 5, which will presently be discussed in more detail.

The user codes, whether they be the initial code or a new code, must be implemented in the key 12 by the key coder 10 also shown in Figure 1, before it can be read by a reader. Referring now to Figure 2, there is

shown the key coder 10 and a key 12 which is to be recorded with a new code. An initial code is provided in the key 12 at all times.

The key coder 10 comprises a keypad 62, which has alphanumeric keys for the inputting of code phrases corresponding to the initial code (current code) and the new code. Also provided is a display 64, which is used to obtain visual confirmation of keystrokes on the keypad 62.

With reference to the flow diagram of Figure 5, the steps in the recoding procedure are as follows. In the recoding operation of a new code in the key 12, the key 12 must be brought into proximity with the key coder 10, and could even be inserted into a slot or recess during the operation.

The procedure requires the owner of the key, inputting the initial (current) code phrase on the keypad 62. The key coder 10 then performs a bit compression routine and transmits the initial (current) code to the key, where it is received at the Tx/Rx component 30. The initial code is passed to the comparator 46. A comparison is made between the received initial code and the initial code stored in register A 26. If there is a match, the comparator 46 signals the key coder 10 to transmit a new code via Tx/Rx component 30, and also enables the gates 66,68.

At the key coder 10, the owner is then prompted to input the new code phrase, which, once manipulated, becomes the new code and is transmitted to the key 12. Once received by Tx/Rx component 30, the new code can pass through the enabled gate 66 to register A 26, with the existing initial code passing through the enabled gate 68 to register B 28. The comparator 46 then disables the gates 66,68. This completes the recording procedure at the key.

The key coder 10 keeps no records of any code phrases, and recoding can only be effected by the owner of the key who knows the current code.

The detailed sequence involved in the normal operation of the system will now be discussed with reference to Figure 3 and to part of the flow diagram in Figure 6.

Figure 3 shows two user code registers A 26 and B 28, together with other components of the electronic key 12, the key reader 14 and the secured means 20. Register A 26 contains the initial code, being the current code, with register B 28 containing a new code relevant to the code changing function.

The reader 14 is activated by the presence of the key 12, as determined by the sensor 25 in the sensing part 27 of the key reader 14. Power for the respective transmitters and receivers of the key 12 and reader 14 is provided within the sensing part 27, and is shown as supply 29.

The key reader 14 then commences operation by generating a random number using a random number generator 32. This random number is encrypted by encryption device 33 using the installed code of the code register 24 as the cipher for the encryption. The data is encrypted data representative of the installed code. The encryption type used may be any suitable secured technique having an encryption algorithm utilising a cipher. In one example, encryption could be using the Data Encryption Standard (DES).

The encryption device 33 passes the encrypted data to a sensing part 27 which transmits the data to the key 12 via a Tx/Rx device 31. The Tx/Rx device 31 is equivalent to the signal receiver 16 and the signal transmitter 17 of Figure 1, which have conveniently been integrated.

The data is received by the Tx/Rx component 30 of the key 12 and is decrypted by the decryption component 34 using the initial (current) code in register A 26 as the cipher for the decryption, then undergoes a process of bit manipulation in the bit manipulation component 36, which, in an example may be a simple bit inversion.

From the bit manipulation component 36, the data is re-encrypted by the encryption component 38 using the initial (current) code contained in register A 26 as the cipher. The re-encrypted data is then passed to the Tx/Rx component 30 for transmission to the reader 14. This data is encrypted data representative of the initial (current) code.

Once the reader 14 receives the data, it is routed via the sensor 25 to be decrypted by the decryption device 40. A reverse bit-manipulation takes place in the bit manipulation device 42, after which a comparison between the random number and the returned random number is made in a comparator 45 which serves, in part, as the equivalent of the signal output means 22 in Figure 1.

If a match is achieved, the comparitor 45 causes control signal 23 to be passed to the secured means 20, thereby causing it to change its secured state enabling the electronic ignition of the vehicle to be activated in the usual way or from the key 12.

In such a way, the actual installed code or the initial code are never transmitted, and a would-be code breaker is required to know the random number used in the encryption before being able to decrypt the data to determine the initial code, which, in any case, is very difficult given the security afforded by the encryption technique.

The random number generated by the random number generator 32 will be different on every occasion that the presence of the key 12 is sensed by the reader 14. Therefore, the current code or new code stored in the key 12 can never be determined from the reader 14.

The reason for having the bit manipulation in both the key 12 and the reader 14 is to avoid the occasion of an electronic mirror attack whereby the encrypted code can be recorded and immediately transmitted back to the reader, thus obtaining operation illegally.

A red led 52 and green led 54 serve a visual function whereby the red led 52 is normally on when there is data transmission between the key 12 and the reader 14. Once a match is achieved, the red led 52 extinguishes and the green led 54 comes on. If normal operation is not achieved, the red led 52 remains on for a fixed period, during which time no further reading occurs. After the expiration of the fixed time, the red led 52 extinguishes, and the user is free to attempt operation again. This function is under the control of sensor 25. If, after a number of attempts, correct operation by matching of codes is not achieved, the sensor 25 causes the reader 14 to close down for a fixed time. It may also be desirable to cause some alarm to operate.

In the instance that only the sensing part 27 is not integral within the secured means, all the encryption, decryption and logic operations would then take place within the secured means 20, and it is virtually impossible for a would-be violator to effect the control signal 23. Similarly, a simple disruption of the connector to the sensing part 27 would not enable the key reader 14 to be bypassed.

In order to describe the special functional features provided by the security system 5, it is useful to consider firstly the structure of the data constituting the user codes stored in register A 26 and register B 28.

Figure 4 shows an example where the total data word is 224 bits in length. The first 112 bits are reserved for register A 26, while bits 113 to 224 are reserved for register B 28. It may be convenient to provide a single register with suitable addressing to either bits 1-112 or 113-224 as appropriate in place of separate registers. Within each half, the data is further broken down into 28 bit sub-fields designated C_{mn}. The first bit of each sub-field is a flag bit F_x, with the remaining bits being op-code.

There are a number of circumstances where it is desirable to change the installed code contained within the code register 24. Using the present example of a motor vehicle, if the vehicle itself is new, it will be delivered to the owner with a known null code provided as the initial code in the key 12 and the reader. It is then necessary to implement a new code in both the key 12 and the reader 14 unique to that owner. This end is achieved by taking a key 12 which has the known null code in register A 26, and adding to that key the new code using the key coder 10, with the result that the known null code gets written to register B 28, and the new user code is written to register A 26. Therefore, the new code is intended to become the next current code.

Once a new code has been stored in register A 26, the key 12 and reader 14 are not code matched, as the reader 14 still has the installed code matching the null (current) code, which is now resident in register B 28. Therefore, the new code must be placed in the code register 24 as the next installed code.

With further reference to Figure 6, the following steps are taken. The key 12 is held in proximity with the sensing part 27 of the reader 14 which interrogates the key 12 as discussed above, having the received random number encrypted by the contents of register A 26 (that being the new code). When it is subsequently determined by the comparator 45 that a code match has not been successful, an internal flag is set and the key reader 14 assumes either that a change of code may be required or that an illegal key is being used, and interrogates the key 12 again, only this time having the encryption performed by the initial code in register B 28. If a match is then obtained in the comparator 45, the code register 24 then obtains the new code from register A 26, by the following procedure.

Upon a match a further flag is set which, when transmitted to the key 12, causes the new code from register A 26 to be passed to the encryption component 38 where it is encrypted using the installed code from register B 28 as the cipher.

This data is then transmitted from the key 12 and is subsequently received and decrypted to recover the new code. The flag previously set has also caused the comparator 45 to enable the gate 70, thereby allowing the new code to enter the code register 24 and become the next installed code.

The key can now continue to be used, as there will now be a match between the next installed code in code register 24 with the new code as the current code in register A 26. It will be appreciated that a number of keys having the same code could be cut simply using the key coder 10.

A further advantageous feature of embodiments is to provide a security system which can be extended from a single user to a multiple user system, wherein there are many keys distributed, and these keys can be

allocated privileged access rights to various secured devices throughout a system, i.e., various security levels.

In the present example, an application of such a multiple user system is to a fleet of vehicles, where one person can have access to many vehicles, while some other person has sole access to one particular vehicle.

In this example, it is necessary to assign the various keys within the system with privileged user status. The information for this function is present only in the installed code held in code register 24, in contrast to other known systems which rely on a centralised control system linked to readers, wherein this centralized control system determines the degree of privilege of the keys distributed through the system.

Other applications of the invention where multiple user may be more evident are building access systems, where certain areas must be restricted.

The multiple user system of this example is achieved by suitable programming of a key coder 10. When the key coder 10 provides a new code to a key 12 which is then to be used to recode a key reader 14, it is the combination of the first three flag bits F1, F2 and F3 which point to the number of access levels of that key 12 and subsequently of the reader 14. It is necessary to install these flags in code register 24 before a multiple user system can be instituted, and this is the only change required by way of implementation. No hardware changes need be effected.

The combination of these three bits designated as F_L specifies the number of access levels, which, when represented as a decimal number, will be either 0, 1, 2 or 3. Each of these access levels has a number of operation levels associated with it, and it is these operation levels which can be chosen by users according to the application.

For F_L=0, there is only 1 operation level, and such a system is suitable for a single private user. In contrast, when F_L=3, there are a possible 16 operation levels.

The structure of the data word as shown in Figure 3 is not limited to a length of 224 bits, nor is it required to be in the format shown in that example.

When a key of a multiuser system is read by a reader 14 it is necessary to obtain concordance only with op-codes at the specific level of privilege. That is, the relevant sub-field in register A 26 must match the respective sub-field held in code register 24. The flag F_L specifies the number of levels applicable, and it is the code register 24 that determines which sub-fields are to match given the number of levels selected.

The bit, F_m, flags the type of master operation required. For F_m=0, knowing the code at one level enables that code to be changed only at that level. For F_m=1, it is possible only for a master key to be used to change all op-codes for all levels.

From the foregoing, particular advantages provided by embodiments of the invention are that a security system can be provided whereby, even if complete details of the system become known, it is very difficult for the system to be defeated. The only variable component in the system is the user code, which is never transmitted in unencrypted form from either the key or the reader. If the owner suspects that the code phrase has become known, then it is a simple matter to recode the key and then install the new code in the reader 14. As the code phrase is of a large number of characters, it should be easy to remember, and it is also very difficult to break.

The reader 14 alone determines whether any key is authorised for a secured device, and the installed code can only every be changed by firstly obtaining a match with the current code. In such an arrangement, there is no need for the central storage of user codes.

The codes stored in registers of a key or a reader can not be read by any means, and are not open to duplication.

In further embodiments, one or more readers can be connected to one or more controllers, so as to provide a multi-secured device environment. Typically, the various controllers could be in a master/slave relationship.

In an industrial application of an embodiment, all component parts of the system are identical at the time of manufacture and fitting, which provides substantial savings in time and materials. All keys and readers can be manufactured having a known null code, which provides for testing before systems are delivered to the end user.

Any number of keys containing the current code can operate one reader and in any sequence. Any number of readers can be operated by one key with which they are code matched.

CLAIMS:

1. A security system comprising:

(a) a key reader including a signal output means, a signal transmitter, a signal receiver, and a code register for storing an installed code, at least a part of the key reader being integral with a secured means and for providing a control signal thereto from the signal output means to change the secured state of said secured means;

(b) an electronic key including a signal transmitter, a signal receiver and two user code registers, a first of the registers being for storing an initial code and the second of the registers being for storing a new code;

the system being operable such that when said key transmits data representative of said initial code to said reader and there is then provided a match between said initial code and said installed code, there will be generation of said control signal from the signal output means to change the secured state of the secured means,

and further being operable such that if said key transmits data representative of said new code to said reader and there is no match between said new code and said installed code, said key can then receive a request from said reader via said signal receiver to tansmit data representative of said initial code to be received by said reader, and if a match is then provided between said initial code and said installed code, said reader will be placed in a mode to substitute said new code for said installed code to form a next installed code, so that following substitution, the system will be code matched.

2. A security system as claimed in claim 1, wherein the system is operable by transmitting data representative of said installed code to said key before said key transmits data representative of said initial code.

3. A security system as claimed in claim 1, wherein said reader further comprises data encryption means to encrypt a representation of said installed code and said next installed code, and data decryption means to decrypt a representation of said initial code and said new code; and

said key further comprises data decryption means to decrypt a representation of said installed code, and data encryption means to encrypt a representation of said initial code and said new code.

4. A security system as claimed in claim 3, wherein said installed code can provide a cipher for said data encryption means and said data decryption means of said reader, and said initial code and said new code can provide a cipher for the data decryption means and said data encryption means of said key.

5. A security system as claimed in claim 4, wherein said reader also comprises a random number generator means which provides a random number to be encrypted by said data encryption means thereby providing data representative of said installed code and whereby a different encrypted representation of said installed code is transmitted for each subsequent operation.

6. A security system as claimed in claim 5, wherein said reader also comprises a bit manipulation means which performs a bit manipulation on the data decrypted by said reader data decryption means, and said key also comprises bit manipulation means which performs a bit manipulation on the data decrypted by said data decryption means in said key.

7. A security system as claimed in claim 1, wherein a data word corresponding to said new code and said initial code comprises a number of data sub-fields, each data sub-field corresponding to a separate level of security whereby the system facilitates for multiple users, the users thereby being variously authorised to access the system only to a certain level of security.

8. A security system as claimed in claim 1, wherein said key can obtain its operating power supply from said reader by means of an electromagnetic transmission.

9. A method of operating a security system having an electronic key and a key reader, to cause a change of a secured state of a secured means, the method comprising the steps of:

(a) encrypting data representative of an installed code present in said reader,

(b) transmitting said encrypted data representative of said installed code from said reader,

(c) receiving said encrypted data representative of said installed code at said key,

(d) decrypting said received data,

(e) encrypting said decrypted data to form encrypted data representative of an initial code present in said key,

(f) transmitting said encrypted data representative of said initial code from said key,

(g) receiving said encrypted transmitted data at said reader,

(h) decrypting said received data,

(i) comparing said decrypted data representative of said initial code with said data representative of said installed code, and

(j) if there is a match, causing generation of an output signal to the secured means to cause the change of its secured state.

10. A method as claimed in claim 9, comprising the further step of bit manipulating said received decrypted data in said key following step (d), and bit manipulating said received decrypted data in the reader following step (h).

11. A method of operating a security system having:

an electronic key and

a key reader which in a normal operation can provide an output signal to a secured means in response to there being code matching between an initial code stored in the key and an installed code stored in the reader whereby the secured means can change its secured state,

the method comprising the steps of:

(a) providing a new code to said key so said key has both said initial code and said new code,

(b) transmitting data representative of said new code from said key,

(c) receiving the data representative of said new code at said reader,

(d) determining if there is a match of said new code with said installed code,

(e) on a mismatch, causing transmission of data representative of said initial code to said reader from said key,

(f) receiving the signal of said initial code at said reader,

(g) determining if there is a match of said initial code with said installed code,

(h) on a match, placing said reader in a mode to substitute said installed code with said new code to form a next installed code,

(i) and thereafter upon operation of the system with the new code, causing said output signal to be provided upon a match with said next installed code.

12. A method as claimed in claim 11, wherein data transmitted between said key and said reader is firstly encrypted by encryption means in both said key and said reader, and data received by both said key and said reader is decrypted by respective decryption means in said key and said reader.

13. A method as claimed in claim 12 comprising the further step of encrypting said new code in said key using said initial code as a cipher, whereby, in said reader, decryption recovers the new code which then becomes the next installed code.

14. A method as claimed in claim 11, wherein the system can provide for multiple users having respective predetermined levels of security, comprising the further steps of:

arranging a data word into a number of sub-fields, and a number of flag bits, whereupon, in operation of the system, the flag bits indicate the level of security of a user.

15. A key for a security system, said key comprising a signal transmitter, a signal receiver and two user code registers, the first of the registers being for storing an initial code and the second of the registers being for storing a new code, and circuit means for permitting said initial code to be replaced by said new code, said circuit means including a comparator and gate means connected therewith, said comparator being for comparing the initial code with a code received by said receiver and upon a match being determined, enabling said gate means so said initial code in said first register will be passed to said second register, said transmitter being operable to transmit data representative of the initial code in said first register for normal operation of said key.

16. A key as claimed in claim 15, wherein said initial code when stored in said second register is accessable for a check with a code matched key reader for said key to enable said key reader to have said initial code replaced with said new code for subsequent operation of said key and said reader with said new code, the key and said reader being operable such that when said key transmits data representative of said initial code to said reader and there is then provided a match between said initial code and said installed code, there will be generation of said control signal from the signal output means to change the secured state of the secured means,

and further being operable such that if said key transmits data representative of said new code to said reader and there is no match between said new code and said installed code, said key can then receive a request from said reader via said signal receiver to transmit data representative of said initial code to be received by said reader, and if a match is then provided between said initial code and said installed code, said reader will be placed in a mode to substitute said new code for said installed code to form a next installed code, so that following substitution, the system will be code matched.

17. A key as claimed in claim 16, further comprising data decryption means to decrypt a representation of said installed code, and data encryption means to encrypt a representation of said initial code and said new code.

18. A key as claimed in claim 17, wherein said initial code and said new code can provide a cipher for the data decryption means and said data encryption means of said key.

19. A key as claimed in claim 18, including bit manipulation means for performing bit manipulation on the data encrypted by said data decryption means.

20. A key as claimed in claim 16, wherein said first and second registers are of sufficient size to store said initial code and said new code together with sub-fields to provide a level of security which may be different to that in other such keys.

21. A key as claimed in claim 16, including electromagnetic power reception means for permitting operating power to be received thereby.

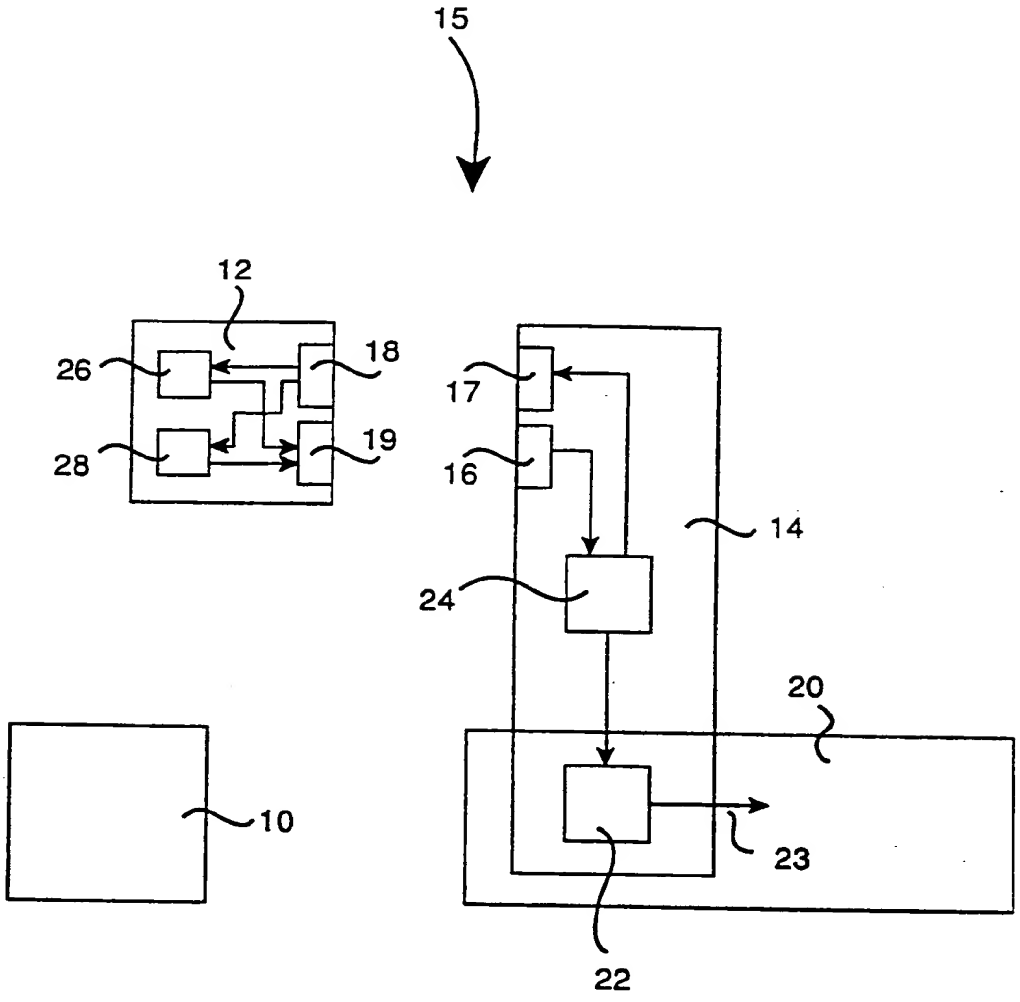


FIG. 1.

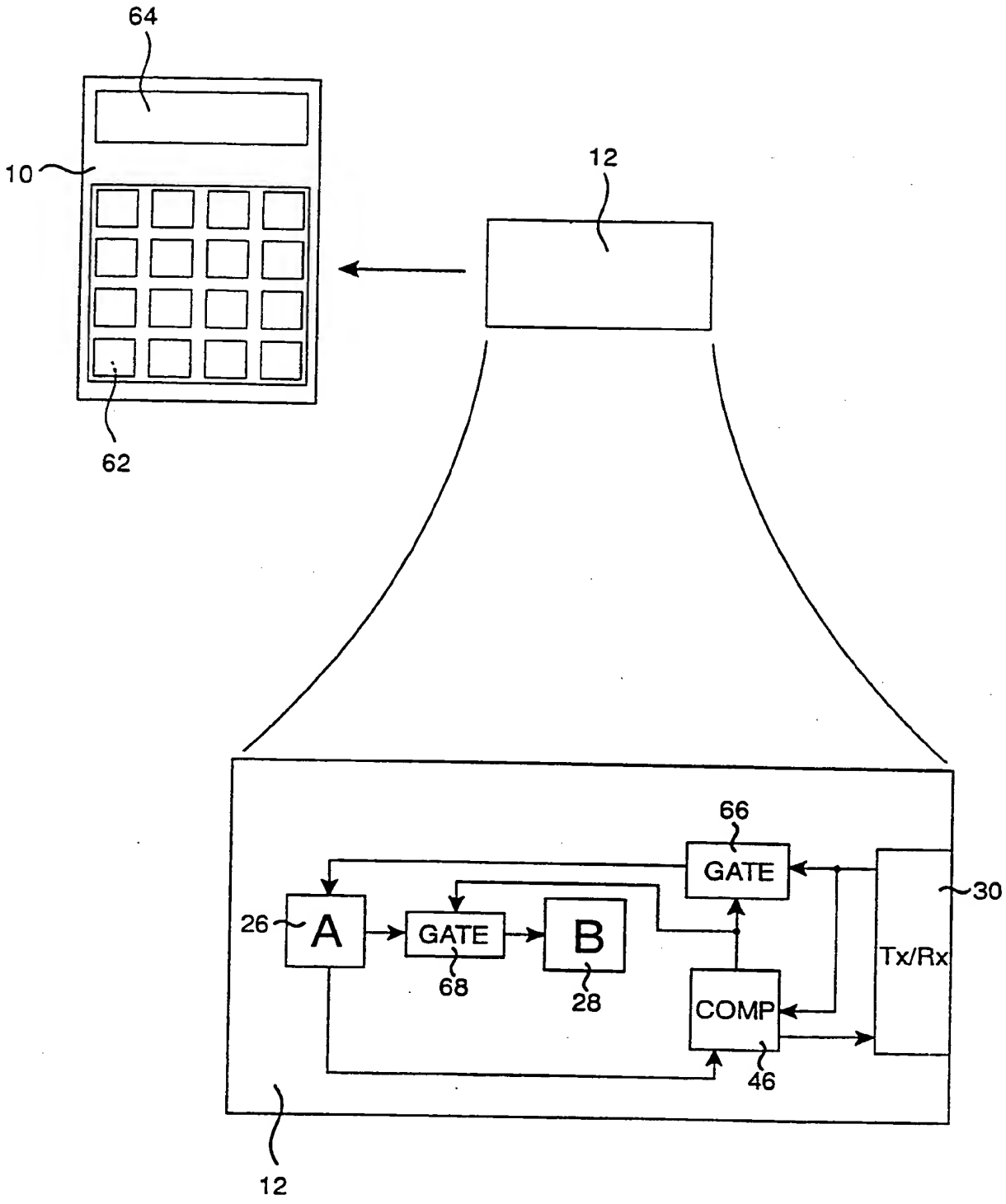


FIG. 2.

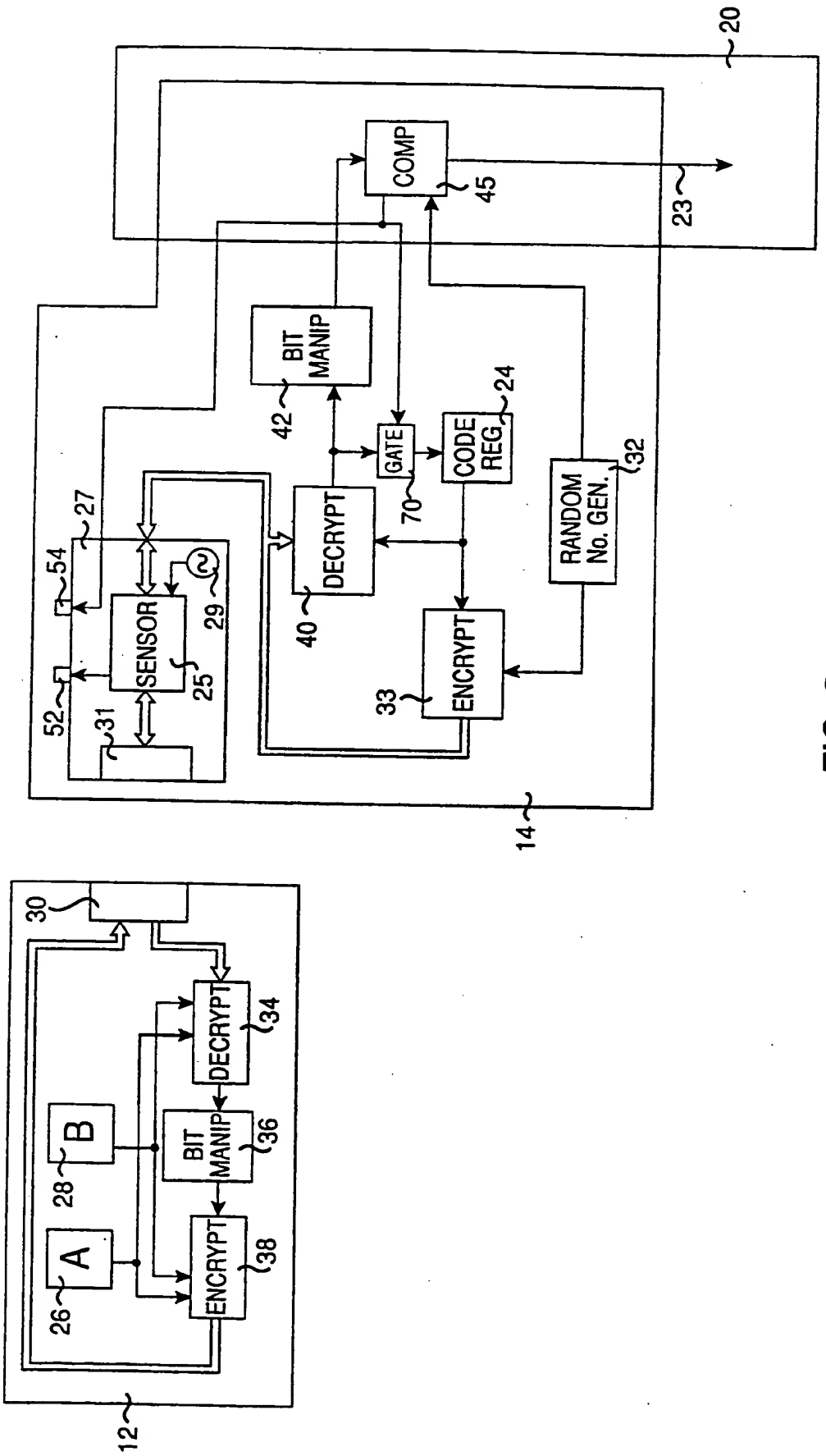

20
COMP
45
23
BIT MANIP
42
GATE
70
CODE REG
24
RANDOM No. GEN.
32
DECRYPT
40
ENCRYPT
33
27
54
SENSOR
25
29
52
31
14
30
DECRYPT
34
B
28
BIT MANIP
36
A
26
ENCRYPT
38
12

FIG. 3.

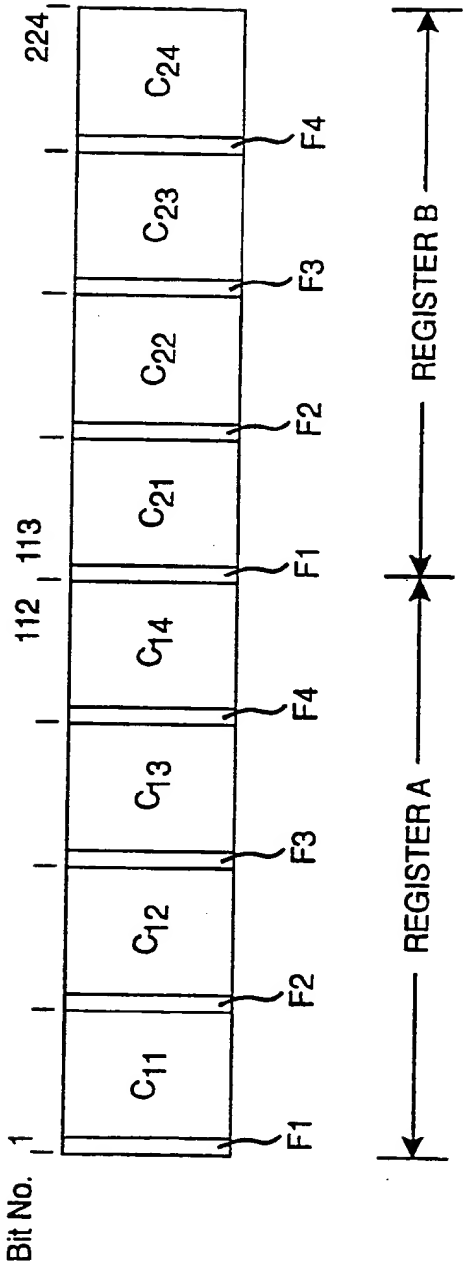

Bit No.
1
112
113
224
C_{11}
C_{12}
C_{13}
C_{14}
C_{21}
C_{22}
C_{23}
C_{24}
F1
F2
F3
F4
REGISTER A
REGISTER B
$F_X = \{F_1, \ldots, F_4\}$
$F_L = \{F_1, F_2, F_3\}$
$F_m = \{F_4\}$
$C_{mn} = \{C_{11}, C_{12}, \ldots, C_{23}, C_{24}\}$

FIG. 4.

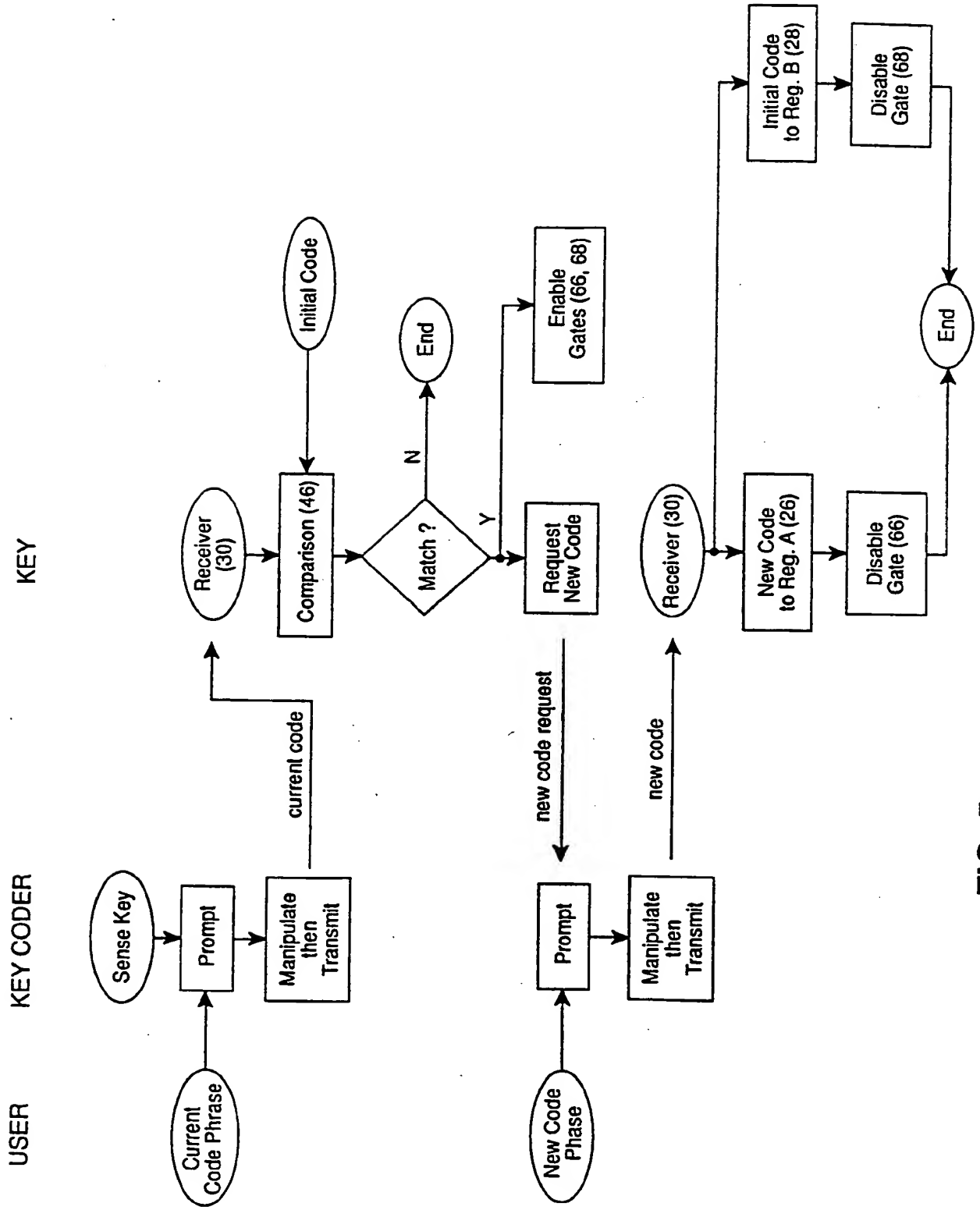

USER
KEY CODER
KEY
Current Code Phrase
Sense Key
Prompt
Manipulate then Transmit
current code
Receiver (30)
Comparison (46)
Initial Code
Match ?
N
End
Y
Enable Gates (66, 68)
Request New Code
new code request
New Code Phase
Prompt
Manipulate then Transmit
new code
Receiver (30)
New Code to Reg. A (26)
Disable Gate (66)
Initial Code to Reg. B (28)
Disable Gate (68)
End

FIG. 5.

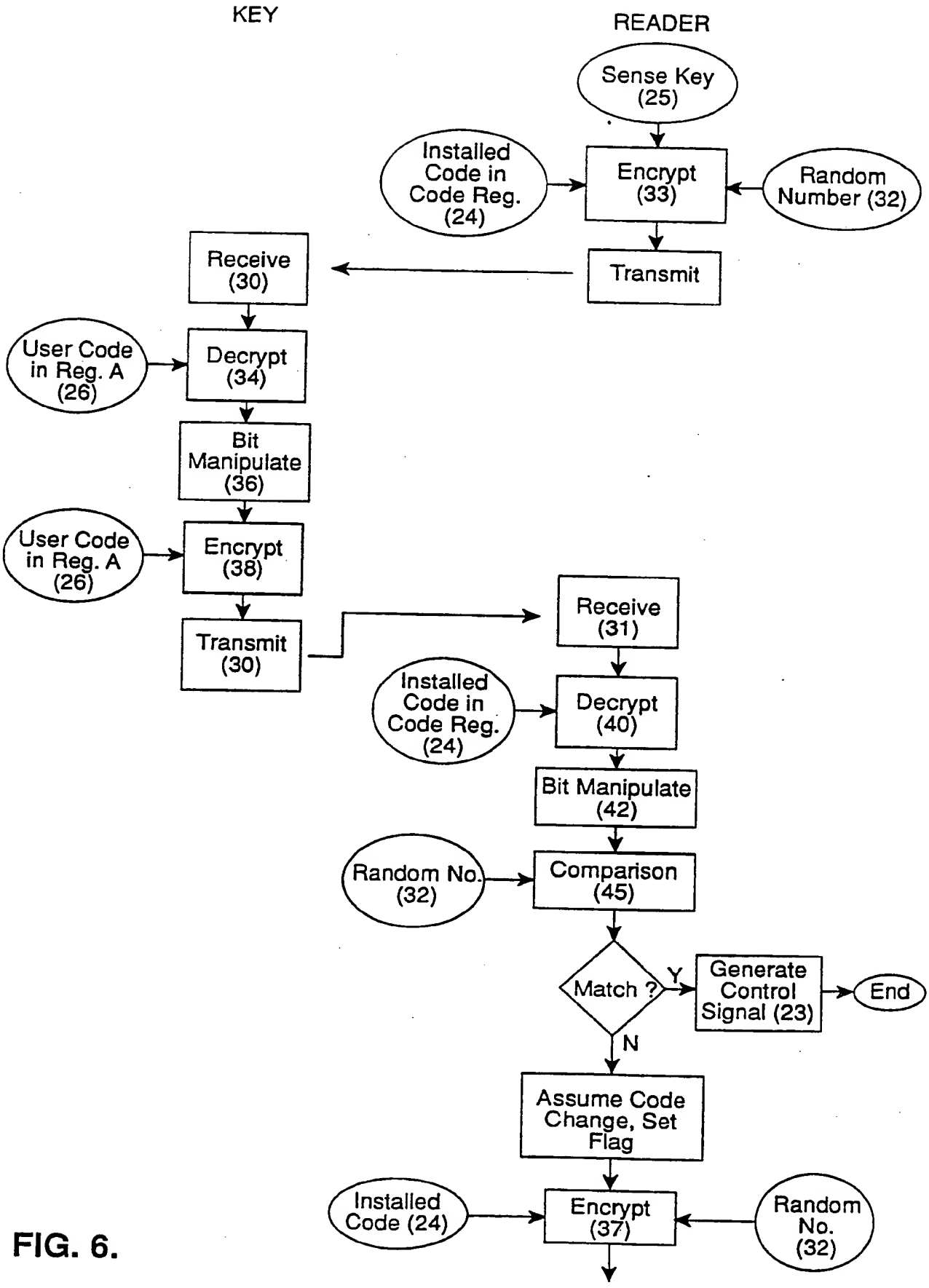

KEY
READER
Sense Key (25)
Installed Code in Code Reg. (24)
Encrypt (33)
Random Number (32)
Transmit
Receive (30)
User Code in Reg. A (26)
Decrypt (34)
Bit Manipulate (36)
User Code in Reg. A (26)
Encrypt (38)
Transmit (30)
Receive (31)
Installed Code in Code Reg. (24)
Decrypt (40)
Bit Manipulate (42)
Random No. (32)
Comparison (45)
Match ?
Y
Generate Control Signal (23)
End
N
Assume Code Change, Set Flag
Installed Code (24)
Encrypt (37)
Random No. (32)

FIG. 6.

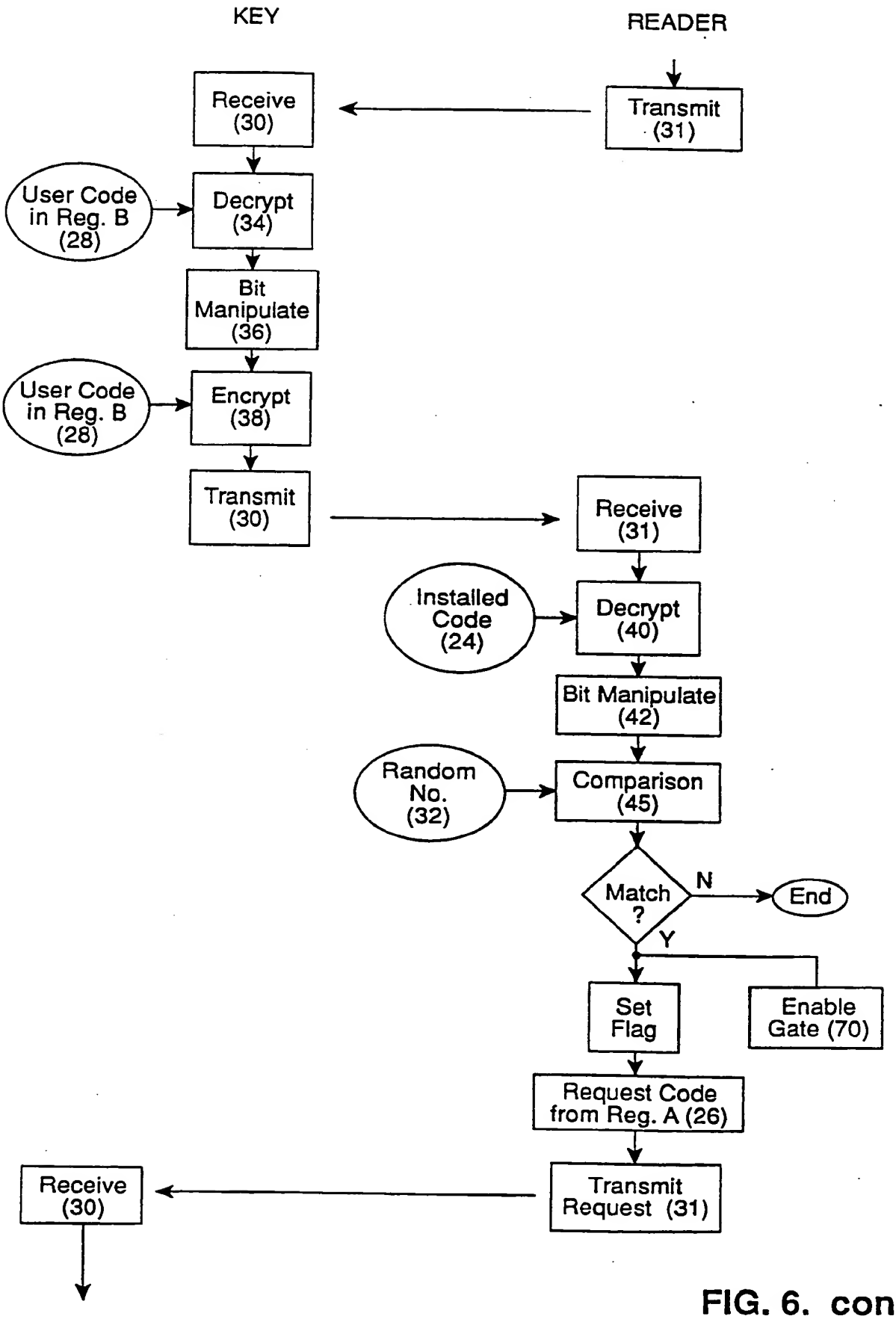

KEY
READER
Receive (30)
Transmit (31)
User Code in Reg. B (28)
Decrypt (34)
Bit Manipulate (36)
User Code in Reg. B (28)
Encrypt (38)
Transmit (30)
Receive (31)
Installed Code (24)
Decrypt (40)
Bit Manipulate (42)
Random No. (32)
Comparison (45)
Match ?
N
End
Y
Set Flag
Enable Gate (70)
Request Code from Reg. A (26)
Receive (30)
Transmit Request (31)

FIG. 6. cont.

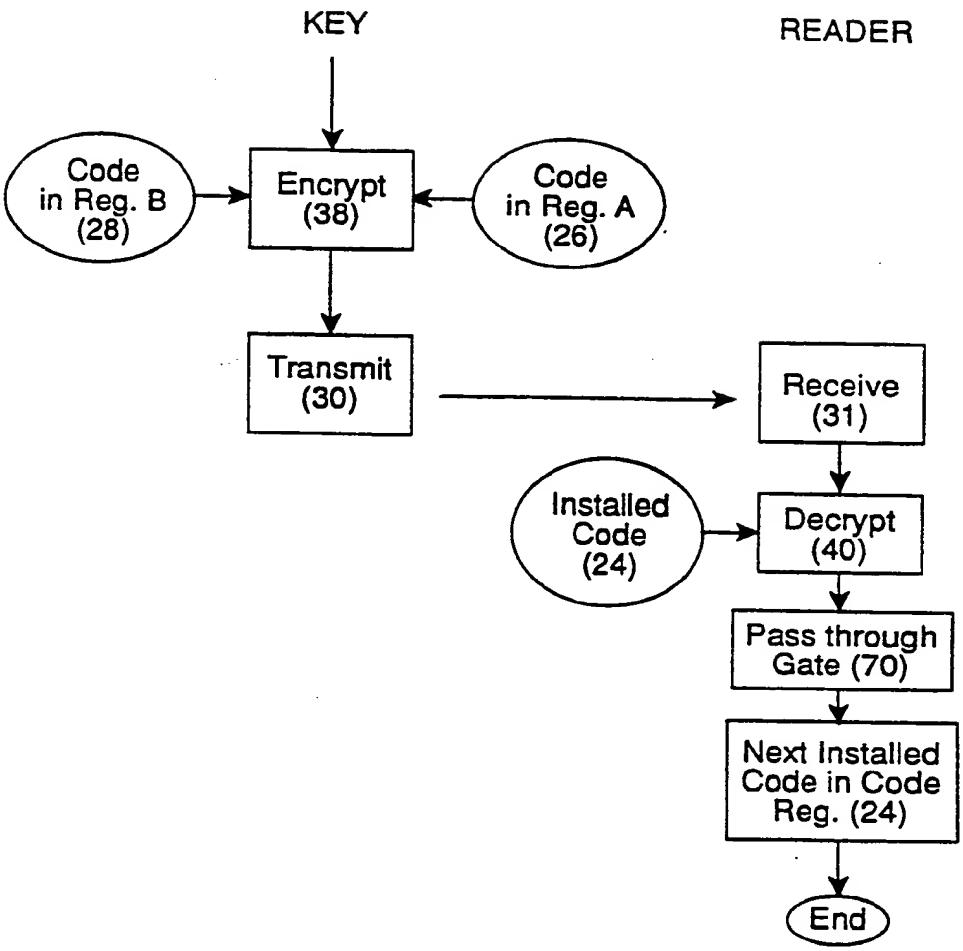

KEY
READER
Code in Reg. B (28)
Encrypt (38)
Code in Reg. A (26)
Transmit (30)
Receive (31)
Installed Code (24)
Decrypt (40)
Pass through Gate (70)
Next Installed Code in Code Reg. (24)
End

FIG. 6. cont.

INTERNATIONAL SEARCH REPORT

International Application No. PCT/AU 90/00235

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) 6

According to International Patent Classification (IPC) or to both National Classification and IPC

Int. Cl.[5] E05B 49/00 G08B 29/00 G06K 19/00

II. FIELDS SEARCHED

Minimum Documentation Searched 7

Classification System	Classification Symbols
IPC[5]	E05B 49/00 G08B 29/00 G06K 19/00

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched 8

AU: IPC as above

III. DOCUMENTS CONSIDERED TO BE RELEVANT 9

Category*	Citation of Document,[11] with indication,[12] where appropriate, of the relevant passages	Relevant to Claim No 13
A	AU,B, 16323/83 (554053) (LEONARD GENEST) 9 February 1984 (09.02.84)	
A	AU,A, 13230/83 (LEONARD GENEST) 20 October 1983 (20.10.83)	
A	US,A, 4519228 (SORNES) 28 May 1985 (28.05.85)	
A	US,A, 4213118 (GENEST et al) 15 July 1980 (15.07.80)	
A	US,A, 3662342 (HEDIN et al) 9 May 1972 (09.05.72)	
A,P	GB,A, 2221714 (JENG-JYI LEE) 14 February 1990 (14.02.90)	
A	GB,A, 2163579 (PA CONSULTING SERVICES LTD) 26 February 1986 (26.02.86)	
A	GB,A, 1467891 (PITNEY ROOWES INC) 23 March 1977 (23.03.77)	
A,P	Patent Abstract of Japan, M932, page 25, JP,A, 63-117053 (BUNKA SHUTTER K.K.) 20 November 1989 (20.11.89)	

* Special categories of cited documents: 10

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
13 August 1990 (13.08.90)	20 August 1990
International Searching Authority	Signature of Authorized Officer
Australian Patent Office	W CLARKSON

Form PCT/ISA/210 (second sheet) (January 1985)

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON
INTERNATIONAL APPLICATION NO. PCT/AU 90/00235

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report	Patent Family Members					
AU 16323/83	BE	897269	DE	3327720	FR	2531128
	GB	2125096	US	4558175		
AU 13230/83	BE	896489	FR	2525268	GB	2118614
US 4213118	CA	1101513	FR	2370308	GB	1597984
GB 1467891	US	3999655				

END OF ANNEX